Subject: Personal Responsibility For Computer Resources

Supersedes: DCS 7.3, 05/01/03

Local Policy: No
Local Procedures: No
Training Required: No
Applicable Practice Model Standard(s): None

Approved by: Linda P. Miller

Effective date: 09/01/97
Revision date: 03/01/05

Application

To All Employees Assigned a Computer With The Department Of Children's Services

Authority:

TCA 37-5-106

Policy

All computers that are property of the Department of Children's Services shall be assigned either a function or to an individual. Each employee who is assigned a computer must read and sign form C*S-0062, Computer Code of Ethics*. Each employee who is assigned a computer is personally responsible for utilization and care of this piece of State property. It is the responsibility of the employee to insure that any other employee using the computer is notified of the personal responsibility.

A. Assignment Of Computer

1. The DCS Office of Information Systems will assign computers to each individual employee of the department as outlined in DCS policy *7.6, Assignment of Computers and Related Equipment*.

2. The employee shall sign form *CS-0062, Computer Code of Ethics* and an *Information Technology Resources and Services Use Agreement* indicating personal responsibility and acknowledging that disciplinary action may be taken for negligence, loss or damage.

B. Security Of Hardware And Software

All State property should be adequately safeguarded at all times and users should be mindful of the threat of fire, theft, and environmental hazards involved in using State property while in their custody.

C. Use Of Computers and Software

1. Assigned computer hardware or software must only be used by authorized DCS employees.

2. Prior consultation and approval must be made with the DCS Office of Information Systems before peripheral components or software can be installed into or connected to any microcomputer or peripheral device.

3. Each section and its employees shall comply with computer software licensing agreements and federal laws, including copyright and patent laws.

4. DCS shall adopt the following practices to control computer software. Department administration shall designate persons who will:

   a) Keep and maintain an inventory control listing of all agency-owned computer software, regardless of the software acquisition cost.

   b) Keep track of all computer software license agreements.

   c) Provide enough legally purchased copies of computer software to enable all employees to meet management's expectations and reduce any necessity for computer software piracy.

   d) Ensure that all data or computer software is removed from the storage media of any computer device before disposition or transfer of equipment, unless computer software and related documentation are included as part of the transfer.

5. Carefully research computer software licensing agreements before purchasing computer software.

6. The Department of Children's Services will measure compliance with this policy by conducting a periodic audit. Agency staff will conduct these audits as directed by the Commissioner.

7. Any employee who is not in compliance with this policy may

be subject to disciplinary action.

D. Use of Laptops

Reference DCS Policy *7.4, Mobile Device Issuance* for procedures.

E. Use of The Internet

Reference DCS Policy *7.2.FA, Acceptable Use, Network Access Rights and Obligations* for procedures.

F. Electronic Mail

Reference DCS Policy *7.2.FA, Acceptable Use, Network Access Rights and Obligations* for procedures.

G. Computer Viruses

1. It is the responsibility of any person accessing the Department's computer environment to ensure that correct and consistent security procedures are followed in order to avoid the accidental introduction of a computer virus into the system.

2. All equipment and software within the Department's computer environment will execute a virus scan product made available through the *Novell-delivered Application* launcher by the Office of Information Resources.

3. Each infestation will be reported to the DCS Office of Information Systems. The following information will be collected and reported in order to properly track and eradicate each occurrence:

   a) Virus Name or Type

   b) Location of the virus

   c) Source of virus (received via email, diskette)

   d) Potential recipients of infected material

   e) Steps taken to disinfect.

Forms

CS-0062 Code of Ethics For Information Systems Management

Collateral Documents

None

Standards

None

Glossary

Term	***Definition***
Computer Virus:	A software program capable of reproducing itself and usually capable of causing great harm to files or other programs on the same computer.